FortiManager - Release Notes

Version 6.0.0

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

July 13, 2018
FortiManager 6.0.0 Release Notes
02-600-474417-20180713

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Supported models 6
Minimum screen resolution 6
What's new in FortiManager 6.0.0 7
SD-WAN Improvements 7
SD-WAN Central Template 7
SD-WAN Monitoring 7
Export IPS and Application Information to a CSV File 7
Export Device List to CSV 7
Find and Replace Objects 8
Fortinet Security Fabric Rating 8
Automatic Policy Package Install for Offline Devices 8
Workspace Device Lock 8
Workflow Improvements 8
AP Manager Floor Map Support 8
Special Notices **9**
ADOM Upgrade for FortiManager 6.0 9
Reconfigure SD-WAN after Upgrade 9
FortiGate VM 16/32/UL license support 9
Hyper-V FortiManager-VM running on an AMD CPU 9
VM License (VM-10K-UG) Support 9
FortiOS 5.4.0 Support 10
SSLv3 on FortiManager-VM64-AWS 10
Upgrade Information **11**
Upgrading to FortiManager 6.0.0 11
Downgrading to previous firmware versions 11
FortiManager VM firmware 11
Firmware image checksums 12
SNMP MIB files 13
Product Integration and Support **14**
FortiManager 6.0.0 support 14
Feature support 17
Language support 18
Supported models 19
Compatibility with FortiOS Versions **26**
Compatibility issues with FortiOS 5.6.4 26
Compatibility issues with FortiOS 5.6.3 26
Compatibility issues with FortiOS 5.6.0 and 5.6.1 26

Compatibility issues with FortiOS 5.4.9 27
Compatibility issues with FortiOS 5.2.10 27
Compatibility issues with FortiOS 5.2.7 27
Compatibility issues with FortiOS 5.2.6 27
Compatibility issues with FortiOS 5.2.1 28
Compatibility issues with FortiOS 5.2.0 28
Resolved Issues 29
AP Manager 29
Device Manager 29
Global ADOM 30
Policy and Objects 30
Revision History 32
Script 32
Services 32
System Settings 33
VPN Manager 33
Workplace and Workflow 33
Others 33
Known Issues 35
AP Manager 35
Device Manager 35
FortiClient Manager 36
FortiSwitch Manager 36
Global ADOM 37
HA 37
Policy & Objects 37
Revision History 39
Script 39
Services 39
System Settings 40
Workspace and Workflow 40
VPN Manager 40
Others 40
Appendix A - FortiGuard Distribution Servers (FDS) 41
FortiGuard Center update support 41

Change Log

Date	Change Description
2018-04-18	Initial release of 6.0.0.
2018-04-19	Added *Special Notices* > *ADOM Upgrade for FortiManager 6.0*.
2018-05-01	Added 5.6.4 support to *Product Integration & Support* > *FortiOS*. Added 5.6.4 section to *Compatibility with FortiOS*.
2018-05-11	Added 5.4.9 support to *Product Integration & Support* > *FortiOS*. Added 5.4.9 section to *Compatibility with FortiOS*.
2018-06-27	Added note to *Product Integration* > *Supported Models* > *FortiGate Models* > *6.0* > *FortiGate Hardware Low Encryption*.
2018-07-13	Updated *Product Integration and Support* > *Language Support* to clarify that you can create your own language translation files for Russian, Hebrew, and Hungarian, and import the language translation files into FortiManager by using the CLI.

Introduction

This document provides the following information for FortiManager 6.0.0 build 0092:

- Supported models
- What's new in FortiManager 6.0.0
- Special Notices
- Upgrade Information
- Product Integration and Support
- Compatibility with FortiOS Versions
- Resolved Issues
- Known Issues
- FortiGuard Distribution Servers (FDS)

For more information on upgrading your device, see the FortiManager *Upgrade Guide*.

Supported models

FortiManager version 6.0.0 supports the following models:

FortiManager	FMG-200D, FMG-200F, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Minimum screen resolution

The recommended minimum screen resolution is 1280 x 800. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

What's new in FortiManager 6.0.0

The following is a list of new features and enhancements in 6.0.0. For details, see the *FortiManager Administrator Guide*:

Not all features/enhancements listed below are supported on all models

SD-WAN Improvements

You can centrally provision SD-WAN templates by specifying SD-WAN interface members, WAN link performance criteria and application routing priority.

Object dynamic mapping is now supported in SD-WAN templates, and the settings defined in the SD-WAN templates can be installed to the managed FortiGates.

SD-WAN Central Template

From the *Device Manager* pane, you can now configure a central SD-WAN template, and then install the settings in the SD-WAN template to multiple FortiGates.

SD-WAN Monitoring

You can now centrally monitor SD-WAN performance:

- Map View displays SD-WAN enabled devices on Google Map with color coded icons. Mouse over to view health performance statistics for each SD-WAN link member
- Table View provides more granular information on each SD-WAN link member such as link status, applications performance and their bandwidth usage.

Export IPS and Application Information to a CSV File

You can export IPS or Application signature information to a CSV file from the *Intrusion Prevention* or *Application Control* profiles under the *Object Configuration* menu.

Export Device List to CSV

You can now export the device list table to a CSV file from the *Device Manager* > *Device & Groups* tab.

Find and Replace Objects

Find and Replace option is now available by right-clicking an object from the policy table. It finds all occurrences of the selected object and allows to replace one or multiple occurrences by one-click.

Fortinet Security Fabric Rating

Security Fabric Rating can now be centrally managed from FortiManager. You can view the summary report of the latest security best practice tests or run tests on demand for the selected security fabric cluster.

Automatic Policy Package Install for Offline Devices

From the *Install Wizard*, the offline devices are now available for a policy package install. If selected, the device database of the offline devices will be updated, and the policy package will be automatically pushed to the devices once they are back online.

Workspace Device Lock

When *Workspace* mode is enabled, you can now apply a lock to one or multiple devices to make configuration changes from the Device Manager.

Workflow Improvements

When workflow mode is enabled, users now have an option to preview their diff before submitting the changes.

AP Manager Floor Map Support

A floor map image file can be imported to the *AP Manager* pane from the *Map View* tab. The managed FortiAPs can then be placed on the floor map for easy monitoring.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.0.0.

ADOM Upgrade for FortiManager 6.0

Upgrade is available for ADOM version 5.0 to migrate to version 5.2, 5.4, and 5.6. Currently, there is no ADOM upgrade option for ADOM version 5.6 to move to version 6.0.

Reconfigure SD-WAN after Upgrade

The SD-WAN module has been fully redesigned in FortiManager v6.0 to provide granular monitor and control. Upgrading SD-WAN settings from 5.6 to 6.0 is not supported. Please reconfigure SD-WAN after upgraded to v6.0.

FortiGate VM 16/32/UL license support

FortiOS 5.4.4 introduces new VM license types to support additional vCPUs. FortiManager 5.6.0 supports these new licenses with the prefixes of FGVM16, FGVM32, and FGVMUL.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

VM License (VM-10K-UG) Support

FortiManager 5.4.2 introduces a new VM license (VM-10K-UG) that supports 10,000 devices. It is recommended to upgrade to FortiManager 5.4.2 or later before applying the new license to avoid benign GUI issues.

FortiOS 5.4.0 Support

With the enhancement in password encryption, FortiManager 5.4.2 and later no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.2 or later.

The following ADOM versions are not affected: 5.0 and 5.2.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
end
```

Upgrade Information

Upgrading to FortiManager 6.0.0

You can upgrade FortiManager 5.6.0 or later directly to 6.0.0. If you are upgrading from versions earlier than 5.6.x, you should upgrade to the latest patch version of FortiManager 5.6, then 6.0.0.

For details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

FortiManager 6.0.0 support

The following table lists 6.0.0 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 59 • Google Chrome version 65 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 6.0.0 • 5.6.4 • FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.6.4 on page 26. • 5.6.2 to 5.6.3 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.2 to 5.6.3, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.6.3 on page 26. • 5.6.0 to 5.6.1 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.6.0 and 5.6.1 on page 26. • 5.4.9 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.9, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.9 on page 27. • 5.4.1 to 5.4.8 • 5.2.8 to 5.2.13 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.10 on page 27. • 5.2.7 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.7 on page 27. • 5.2.6 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.6 on page 27. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.1 on page 28. • 5.2.0 FortiManager 6.0.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility issues with FortiOS 5.2.0 on page 28.
FortiAnalyzer	• 6.0.0 • 5.6.0 to 5.6.3 • 5.4.0 to 5.4.4 • 5.2.0 to 5.2.10 • 5.0.0 to 5.0.13

FortiAuthenticator	• 5.2.2
FortiCache	• 4.2.7 • 4.2.6 • 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 5.6.6 • 5.6.3 • 5.6.0 • 5.4.0 and later • 5.2.0 and later
FortiMail	• 5.4.5 • 5.4.2 • 5.3.7 • 5.2.9 • 5.1.6 • 5.0.10
FortiSandbox	• 2.5.1 • 2.5.0 • 2.4.1 • 2.4.0 • 2.3.2 • 2.2.1 • 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.9.0 • 5.8.6 • 5.6.0 • 5.5.4 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6

FortiDDoS	• 4.5.0 • 4.4.1 • 4.2.3 • 4.1.11 Limited support. For more information, see Feature support on page 17.

Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS
	• Citrix XenServer 6.2
	• Linux KVM Redhat 6.5
	• Microsoft Azure
	• Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2
	• OpenSource XenServer 4.2.5
	• VMware
	  • ESX versions 4.0 and 4.1
	  • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5

To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiAuthenticator			✓	✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages and import the language translation files into FortiManager by using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
     <password> <file name>
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
     <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
     <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information about commands, see the *FortiManager CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.0.0.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-60E-DSL, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C,FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1 **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.6

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE,FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1 **FortiGate 7000 Series:** FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC **FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM **FortiGate Rugged:** FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3800D-DC, FCR-3810D-DC, FCR-3815D-DC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.6
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.0 2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-2000E	5.6.0
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.8
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E, FAC-VM	4.0 and 4.1

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 6.0.0.

Compatibility issues with FortiOS 5.6.4

Bug ID	Description
486921	FortiManager may not be able to support the syntax for the following objects: • `rsso-endpoint-block-attribute`, `rsso-endpoint-block-attribute`, or `sso-attribute` for RADIUS users. • `sdn` and its `filter` attributes for firewall address objects. • `azure` SDN connector type. • `ca-cert` attribute for LDAP users.

Compatibility issues with FortiOS 5.6.3

Bug ID	Description
469993	FortiManager has a different default value for switch-controller-dhcp-snooping from that on FortiGate.

Compatibility issues with FortiOS 5.6.0 and 5.6.1

Bug ID	Description
451036	FortiManager may return verification error on `proxy enable` when installing a policy package.
460639	FortiManager may return verification error on `wtp-profile` when creating a new VDOM.

Compatibility issues with FortiOS 5.4.9

Bug ID	Description

486592	FortiManager may report verification failure on the following attributes for RADIUS users:
	`rsso-endpoint-attribute`
	`rsso-endpoint-block-attribute`
	`sso-attribute`

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 6.0.0 and FortiOS 5.2.10.

Bug ID	Description
397220	FortiOS 5.2.10 increased the maximum number of the firewall schedule objects for 1U and 2U+ appliances. As a result, a retrieve may fail if more than the maximum objects are configured.

Compatibility issues with FortiOS 5.2.7

The following table lists interoperability issues that have been identified with FortiManager version 6.0.0 and FortiOS 5.2.7.

Bug ID	Description
365757	Retrieve may fail on LDAP User Group if object filter has more than 511 characters.
365766	Retrieve may fail when there are more than 50 portals within a VDOM.
365782	Install may fail on system global optimize or system fips-cc entropy-token.

Compatibility issues with FortiOS 5.2.6

The following table lists interoperability issues that have been identified with FortiManager version 6.0.0 and FortiOS 5.2.6.

Bug ID	Description
308294	1) New default wtp-profile settings on FOS 5.2.6 cause verification errors during installation. 2) FortiManager only supports 10,000 firewall addresses while FortiOS 5.2.6 supports 20,000 firewall addresses.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 6.0.0 and FortiOS version 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263896	If it contains the certificate: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` may not work as expected.

Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 6.0.0 and FortiOS version 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.
226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 6.0.0. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
395156	SSID configuration changes may not trigger installation.
457080	Search results within Rogue AP page may display signal in JSON format.
460009	Search results within Managed AP page may disaly Connected Via in JSON format.
465297	Users may be unable to add more than one entry to MAC Address Access Control List under *WiFi Templates* > *SSID*.

Device Manager

Bug ID	Description
305141	The messages may be unclear when there are import errors during an import policy.
397685	FortiManager may create extra interface during installation for hardware switch.
371154	In a Policy Package re-install, the devices selections may change after users do a preview.
437122	The FortiGuard page in Device Manager may be inconsistent with that on FortiGate.
459288	FortiManager may install `last-updated` for certificates thus causing installations to fail.
456751	FortiManager may enable log memory for 5.2.2 FOS devices.
440406	VDOMs in TP mode may be shown as NAT in Device Manager.
459319	Registered devices may be not shown on AWS platform.
450186	After saving an interface page, its dynamic mappings may be deleted.
458969	Selecting a Phase 1 in the Phase 2 Configuration page may reset other settings in this page.
457397	Installation may fail when the name of a CA certificate contains spaces.
458825	Changes in central SD-WAN status check profile may not trigger a configuration status change.

Bug ID	Description
455541	*WAN Link Load Balance >Status Check Profiles* may not be configured.
453391	Users may not be able to map an interface to a Zone if it has been mapped before.
414117	There may be no warnings when users change FortiGate HA sequence.
450195	Some VDOMs may be not displayed in Device Manager for multi-VDOM FortiGates.
458688	VXLAN over IPSec configurations may be not imported.
460412	Managed devices placed in a group in Device Manager are not sorted alphabetically.
461853	Not all Phase 2's are displayed in *Query:IPsec VPN*.
478625	Users may fail to add a static route to a TP VDOM from FortiManager.
470442	HA cluster has members which should not be in the same cluster.
479591	Policy package diff may not work for VDOMs.

Global ADOM

Bug ID	Description
461564	Global ADOM policies may display as `any:any:gall:gall:galways:gALL:Deny` after upgrade.
460002	Global Policy Package inspection mode may be default to Proxy mode.

Policy and Objects

Bug ID	Description
448618	Verification may fail when there is Web Filter local rating with a trailing slash created in FortiManager.
439086	The sequence ID of a policy may changed after users drag an object to a column.
458131	UUID may be pushed in every installation.
411805	Search function may not work for *Section Titles*.
459268	Copy and paste multiple firewall policies between policy packages may result in an unexpected reorder of the rules.
460136	Dragging an object under Dual Pane mode may put the object into a policy unexpectedly.

Bug ID	Description
459644	Newly created firewall address from the right pane may replace a firewall address in the source address selection.
444883	After users collapse a section in Policy Package list, the focus may go up to the top.
456155	Users may need to refresh the page to see the update if they try to copy a policy from a package and paste it to another.
456765	Users may not be able to add custom IPS signatures with `—dns.query_type`.
452008	Renaming a section may create a new one.
435107	FortiManager may install a new Web Filter entry at the end of the URLfilter table.
457938	Service group changes may be not installed to FortiGates.
453744	FortiManager may accept a wildcard address for URL filters when the type is set to simple.
457084	Changes in a firewall object may not trigger all of the referenced policies status to change to *Modified*.
441222	More than 16 ranges may be allowed in service in FortiManager.
456748	Selecting a FortiGate device may not have all of its VDOMs selected in policy package install.
459281	Search in Policy Package may yield UUID results even when the UUID column is hidden.
417723	Removing the last object in an attribute may not replace it with the *None* object.
459000	When there is a large number of Policy Packages, the search function may freeze the browser.
381161	Duplicate address objects with different comments may be deemed as different.
459769	Users may not be able to edit address groups and schedule profiles in Policy list page via right click.
460136	Dragging and object under Dual Pane mode may put the object into a policy unexpectedly.
478478	There may be security console crash after users import a large number of URL filters.
461155	Users may fail to create a dynamic interface mapping for dedicated-to-management interface.
396422	Users may not be able to search for Address Objects with CIDR notation in the Policy View.
410239	Clicking on an entry in where used results may not highlight the policy.
461691	Users may fail to create a policy using an address group with an address object that has overlapping name.
477676	The displayed sequence number of a policy may change after inline editing.
459272	Users may not be able to copy multiple firewall policies with multiple section titles.
462561	Policy import may fail due to invalid object of firewall address tags.
436907	The toggles status of Policy Packages may not be remembered.
421016	Users may be unable to select more than one interface in pop up Edit page for a Zone.

Bug ID	Description
307891	Interface selection list in *Create new policy* page may be not filtered.
417358	In Policy Object page, the search result may be lost after users edit an object from it.
442727	Internet-service-id may not match between FortiManager and FortiGate.
444839	Import wizard may incorrectly display that objects are to be updated.
461752	Comment column width under Policy tab may not be re-sized.
410123	Authenticate method negotiate of explicit proxy policy may be missing.
371069	Section view may be enabled when there is a policy using any as an interface.
462880	Importing a urlfilter with \ in a regex type URL may stop responding.
466597	Policy package with / in its name may be invisible.
477105	GUI may be no refreshed upon a negate operation.
475139	The focus may return to the top of the policy list upon a section title operation.
466758	`tcp-portrange` and `udp-portrange` settings are missing on GUI in proxy type service.

Revision History

Bug ID	Description
474231	FortiManager cannot install policy package when external interface is a SD-WAN interface.
474135	Install may fail when configuring IPv6 static routes on FortiGate 6.0 device.

Script

Bug ID	Description
417075	The *Cancel* button in the run script popup may be misleading.

Services

Bug ID	Description
458960	The FortiGuard license status for a device may be incorrect in FortiManager.

System Settings

Bug ID	Description
457906	LDAP authentication may fail for group matching issues.
469142	DST for Mexico City may be incorrect.

VPN Manager

Bug ID	Description
457093	SSL-VPN portal changes may not be installed to FortiGates.
459924	VPN interfaces may not be shown in the drop down list in interface mapping if Zones are disabled in VPN manager.
479257	VPN Manager may allow users to select Zones or irrelevant interfaces as Default VPN Interface.

Workplace and Workflow

Bug ID	Description
459520	When users are in workspace and dual pane mode, the GUI may not show the ADOM object list if the user did not lock the ADOM before they enter the Policy & Objects page.
460672	Policy package status may not change when Workspace mode is enabled.
476205	Ipsec P1/P2 proposals are not displayed when Workspace is enabled and ADOM is not locked.

Others

Bug ID	Description
457762	It may take longer than usual for users to switch between the Device page and the Policy Package page.
439851	IPSec VPN query may not show tunnel status.
459290	Users may not be able to use the ENTER and ESC keys for OK and Cancel operations in the GUI.

Bug ID	Description
473376	FortiManager 6.0.0 is no longer vulnerable to the following CVE References: • CVE-2015-9251

Known Issues

The following issues have been identified in 6.0.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
464811	Updated AP name may get reverted back to its default name if users do not install the change in a while.
462857	Following changes in an AP profile, FortiManager may install unrelated local user group and radius server to VDOM root.
450434	FortiManager may unset `wtp-mode` after users change AP config from AP Manager.
481651	`fapc-compatibility` may be unset.

Device Manager

Bug ID	Description

468776	FortiManager may not be able to add FortiGate 6.0 devices with VDOM enabled.
	Workaround: In each of the configured VDOM, please unset the following configurations for each of the wireless controller's UTM profiles, e.g.,
	`config wireless-controller utm-profile`
	`edit "g-wifi-default"`
	`unset ips-sensor "g-wifi-default"`
	`unset application-list "g-wifi-default"`
	`unset antivirus-profile "g-wifi-default"`
	`unset webfilter-profile "g-wifi-default"`
	`unset firewall-profile-protocol-options "g-wifi-default"`
	`unset firewall-ssl-ssh-profile "g-wifi-default"`
	`next`
	`end`

473491	Certificate Enrollment may fail using SCEP on Microsoft NDES server.
480290	Users may not be able to move aggregated interfaces between VDOMs.
463169	`set apn` is not available in device db under `system lte-modem` for FortiWifi-30E-3G4G-INTL.
467773	All zones are displayed in every FortiGate.

Bug ID	Description
479258	After adding and importing a new device, other device may have *Modified* policy package status.
477009	VM Meter may not show both Master and Slave licensing information on GUI.
474893	Users may be unable to setup multiple passive-interface in OSPF on GUI.
459858	All cluster members are shown as Slave in Logging FortiGates.
475483	Users may fail to use named address in static route configuration.
411968	Users may not be able to configure Replacement Messages and Images for VDOMs.
474621	After users upgrade a v5.2 FortiGate to v5.4 in a v5.2 ADOM, the next installation may fail.
462851	`ha-direct` is not available for SNMP v3 in provisioning templates.
408183	Changing monitored interface status up/down may cause installation to fail.
445537	ADOM version inconsistency warning may be displayed when users add a FortiAnalyzer.
460403	FortiManager may not be able to automatically generate an interface of type `vxlan`.
477142	Cloning a DHCP server may fail at the first attempt.
484229	When enabling or disabling FortiGate's VDOM mode via FortiManager, it may return failure when installing the change. **Workaround:** Enable or disable VDOM mode on FortiGate directly.
485756	FortiManager cannot manage EMAC-VLAN related configurations.

FortiClient Manager

Bug ID	Description
480813	FortiManager may be unable to update definitions for FortiClient when FortiClient is sending vulnerability statistics.
377095	Users may be unable to move FortiClient profile from GUI.

FortiSwitch Manager

Bug ID	Description
483414	Users may be unable to upgrade FortiSwitch from FortiManager.
480294	Installation of FortiSwtich template changes may fail.

Global ADOM

Bug ID	Description
482925	*Internet Service* destination is not displayed in IPv4 Header/Footer Policy in Global ADOM.
470486	Automatic-Install may fail to detect changes to push to ADOMs.

HA

Bug ID	Description
463853	FMG-VM slave may be failed to keep sync when FortiGate configuration is modified on FMG-VM master.
480462	FMG Slave may be failed to sync when users add a bunch of admin users on the Master.
483229	Locking an ADOM on Slave FortiManager may lock the ADOM on the Master FortiManager.

Policy & Objects

Bug ID	Description
481991	The NAT checkbox may be always unchecked in Central SNAT policy.
475241	Users may be unable to clone a global assigned object in local ADOMs.
456710	Searching an IP address in policy list may not yield the result of all the address groups with reference to it.
475496	Source addresses, destination addresses and services may not be listed in alphabetical order in policy list.
482361	After users rename a section, there may be one policy left under the old section name.
474849	The page may return to policy 1 after users insert a policy.
462712	Page jumps might occur when using the middle mouse to scroll through large tables of data in the GUI with Firefox browser.
459314	Users are able to delete used firewall objects.
475594	Users may be not able to create new firewall service custom objects because of the tablesize limit.
481560	There is no validation check for FQDN addresses.

Bug ID	Description
474629	Security Profile Groups created on FortiManager may be pushed to all FortiGates upon next policy installation.
463920	The address searched is not highlighted in address groups.
444671	GUI may hide `logtraffic-start` settings when users check the *No Log* option.
453702	Users may be unable to filter policies with Hit Count, Bytes, Packets, First Used or Last Used.
480389	Import wizard may hang at interface mapping page.
465620	`log-attack-context` is not visible in Intrusion Prevention.
481034	Policy Package installation may fail when a Firewall Policy contains a VIP Group mapped to a zone interface.
470539	Users may be unable to delete some invalid Web URL filters.
475935	FortiManager may falsely report conflicts of `icmptype` and `icmpcode` during policy import.
459655	`per-device` mapping firewall address value changes may not change policy package status to *Modified*.
473104	Some ports in custom service may not get installed to FortiGate.
473973	Drag and drop allows co-existing profiles and profile groups in one single policy.
471030	FortiManager allows users to use wildcard entries under Web Rating Overrides.
460615	Renaming RADIUS server used by Authentication in `Device Manager - Device Name - Interface type WiFi SSID` may not work.
474270	`monitor-mode` option is not available in `gtp` profile.
469657	Policies can be dragged and dropped to outside of visible area.
463662	Users may be unable to move columns.
450922	IPS sensor with more than 8192 signature entries may be created.
484792	After editing an object, an error *Not Found* may occur.
477298	Radius changes may not be pushed to FortiGate if radius user group is IPSec Phase1 VPN.
472825	Web Filter profile may not be changed in Explicit Proxy Policy when profile name contains `+`.

Revision History

Bug ID	Description
472443	FortiManager may not be able to retrieve some profiles when VDOM is enabled on a FortiGate 6.0 device.
478606	The preview of a VDOM with no commands to be installed may show commands to be installed from other VDOMs in a policy re-install.
480723	There may be copy fails when a webfilter and a URL filter share the same name.
477677	There may be copy fails when there is a global range CA certificate.

Script

Bug ID	Description
482929	Users may be unable to add/edit script details using IE 11.
482939	When users run scripts to edit an aggregated interface, extra `unset member` may be added during installation.
471661	*Advanced Device Filters* may be displayed when users are editing CLI script.
480982	Progress bar for installing script may not work if the admin user has *None* access to `import-policy-packages`.

Services

Bug ID	Description
478050	*FortiGuard* > *Package Management* > *Service* page may show duplicate entries after FortiGate HA cluster failover.
475033	Signature packages may be updated every hour when it is set to *update daily*.
483670	FortiManager may not download the image from FortiGuard to upgrade the FortiGate's firmware. **Workaround:** Run the `diagnose fwmanager service-restart` CLI command and perform the upgrade again.

System Settings

Bug ID	Description
481018	DST change may be incorrect for Israel.
476905	Too many event logs may be generated when the policy hit count feature is enabled.
471742	SNMP Request Uptime may not be accurate.

Workspace and Workflow

Bug ID	Description
478444	Policy package status may not change to “Modified” in workflow mode.

VPN Manager

Bug ID	Description
478536	FortiManager may fail to install a recreated VPN with a different name.
470511	Search results may be lost after users cancel from editing an entry in the results.
472726	Users may not be able to add/edit bookmarks in VPN manager when workflow mode is enabled.

Others

Bug ID	Description
469405	The process `uma_upd` may crash often.
481763	`diagnose cdb upgrade check` may not fix all errors for `objcfg-integrity`.
480080	Unsetting adom-mode in config system global does not make adom-mode normal.
471095	ADOM upgrade may fail because of webfilter url filter.
480577	GUI may get stuck at *Temporarily Unavailable* upon upgrading.
483204	FortiManager-3900E may fail to manually negotiate port speed/duplex.
480551	SNMPwalk may fail with error *Error: OID not increasing: IP-MIB::ipAdEntAddr.*

Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• 5.0.0 and later • 5.2.0 and later • 5.4.0 and later • 5.6.0 and later	✓		✓	
FortiClient (Windows)	• 4.3.0 and later	✓			
FortiClient (Windows)	• 4.2.0 and later	✓	✓		✓
FortiClient (Mac OS X)	• 5.0.1 and later • 5.2.0 and later • 5.4.0 and later • 5.6.0 and later	✓		✓	
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 and later • 5.1.0 and later • 5.2.0 and later	✓	✓		
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later	✓			

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiWeb	• 5.0.6 • 5.1.4 • 5.2.0 and later • 5.3.0	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```